Implementation of PSEC-KEM in Hardware and Software

Test and Performance Document

Version 1.0

Sujoy Sinha Roy, Chester Rebeiro and Debdeep Mukhopadhyay
Indian Institute of Technology Kharagpur
West Bengal

27^{th} February 2011

Contents

©NTT Corporation, IIT Kharagpur, 2011

1 Introduction

This document describes the plan for testing and performance of the hardware and software implementations of PSEC-KEM.

1.1 Goals and Objectives

There are two goals for the testing. First is the functional testing of the softare. Second, the measurement of the performance.

1.2 Scope

1.2.1 Software

- PSEC-KEM has two parts : Encryption and decryption. The functional correctness is checked by the correct decryption of the encapsulated key.
- Computation time is measured using the *clock_gettime* function with *CLOCK_REALTIME* option.

1.2.2 Hardware

- The functional correctness is checked by comparing the results obtained with the software implementation for both encryption and decryption.
- The performance results reported in this document are obtained from post place and route results from Xilinx ISE Version 11.1.

1.3 Test Environment

1.3.1 Hardware Testing

Results reported are as obtained from the Xilinx ISE tool (version 11.1) reports. Onboard testing of encryption and decryption hardware was performed on Xilinx Virtex V FPGA XUPV5-LX110T.

1.3.2 Software Testing

PC platform with Intel Core 2 Duo, Linux OS (64 bit), GCC.

1.4 References

[1] Design Document for Implementation of PSEC-KEM in Hardware and Software.

[2] Digilent, *Xilinx XUPV5-LX110T Evaluation Platform*, *http://www.xilinx.com/univ/xupv5-lx110t.htm*

[3] C. Rebeiro, S.S. Roy, D.S. Reddy and D. Mukhopadhyay, "Revisiting the Itoh-Tsujii Inversion Algorithm for FPGA Platforms", IEEE Transactions on VLSI Systems, vol. PP Issue:99 (pre-print).

2 Test Reports

2.1 Hardware Testing

Here we present area and timing report of the PSEC-KEM hardware. The reports are taken from Xilinx ISE (Version 11.1). Area and timing reports are presented in Table 1.

Components	Resources Utilized (Slices)	Freq (MHz) (f)	Clock Cycle (c)	Latency μsec (c/f)	Throughput (per sec) (f/c)
Encryption (Random curve)	44807	38.4	4900	128	7812
Decryption (Random curve)	44623	38.2	4900	128	7812
Encryption (Koblitz curve)	48720	31.8	2500	80	12500
Decryption (Koblitz curve)	47947	31.7	2500	80	12500
Field Multiplier	21216	–	–	–	–
KDF	2748	112	$65 - 195$	$0.6 - 1.8$	555555-1666666

Table 1: Area and Timing for different components of PSEC-KEM in Xilinx Virtex V FPGA

The validation of the hardware was initially planned on the SASEBO GII side channel evaluation board. This board has a Xilinx XC5VLX50 FPGA, which has only 28800 LUTs. Since, our designs for encryption and decryption requires several more LUTS, we were not able to perform on-board testing of encryption and decryption designs using the SASEBO board.

The functional correctness of encryption and decryption components of PSEC-KEM were tested using Modelsim simulation. Behaviorial and Post-Route simulations were correct for both encryption and decryption components. For on-board testing, we have used Xilinx XUPV5-LX110T FPGA kit[2]. The board uses Xilinx Virtex 5 FPGA XC5VLX110T FPGA having around 69000 LUTs. This is sufficient for either the encryption or decryption components of PSEC-KEM in $GF(2^{283})$. We have successfully tested the encryption and decryption hardware in this board.

2.1.1 Performance Metric in Hardware

We measure the performance of the encryption and decryption hardware by the metric

$$Performance = \frac{1}{(Area \times Delay \times ClockCycles)}$$

Area is measured in terms of number of LUTs consumed. When encryption and decryption operations use ECCP defined over random curves, performance of both encryption and decryption hardware are 17.44%. When Koblitz curve based scalar multiplier is used, then performance of both encryption and decryption hardware are 25.7%. Table 2 shows estimated performance of PSEC-KEM encryption or decryption hardware for the fields $GF(2^{163})$ and $GF(2^{233})$ on Virtex V FPGA.

2.1.2 Scaling of PSEC-KEM Hardware in other Galois Fields

In PSEC-KEM encryption and decryption, only the elliptic curve scalar multiplication and modular reduction are dependent on the field $GF(2^m)$. In this section we present an estimate of area and frequency for some of NIST recommended binary random fields. In $GF(2^{283})$, the scalar multiplier for the random curve has an area of nearly $41,000$ LUTs and a frequency of nearly $41MHz$ in Virtex V FPGA. So, without the scalar multiplier, both encryption and decryption hardwares have area of nearly 4000 LUTs. This is a constant overhead which is independent of the size of the finite field used. Additionally, the critical delay path of both encryption and decryption hardwares is through the scalar multiplier and thus the delay of PSEC-KEM encryption or decryption hardware is approximately equal to the delay of the scalar multiplier. Thus, from area and delay of the scalar multipliers in other Galois fields, it is possible to estimate the area and delay of the entire PSEC-KEM. We have implemented elliptic curve scalar multipliers in $GF(2^{163})$ and $GF(2^{233})$ using random curves. From experimental results of scalar multipliers in these fields, we have tried to estimated area and frequency for PSEC-KEM encryption and decryption architectures in fields $GF(2^{163})$ and $GF(2^{233})$. In

Field	Estimated Area (LUTs)	Estimated Freq (MHz) (f)	Clock Cycle (c)	Estimated Latency μsec (c/f)	Estimated Performance (%)
$GF(2^{163})$	18000	41	2900	70	79
$GF(2^{233})$	28000	43	4030	94	38

Table 2: Estimated Performance of PSEC-KEM on Xilinx Virtex V FPGA for other fields

Figure 1, a graph shows estimated area of PSEC-KEM hardware for two other Galois fields $GF(2^{163})$ and $GF(2^{233})$ along with actual area for $GF(2^{283})$.

Similarly in Figure 2, the graph shows estimated frequency for PSEC-KEM in $GF(2^{163})$ and $GF(2^{233})$ along with actual frequency for $GF(2^{283})$.

From Figure 2, it can be seen that the operational frequency in $GF(2^{233})$ is expected to be higher compared to $GF(2^{163})$ and $GF(2^{283})$. This happens because the field $GF(2^{233})$ is generated by an irreducible trinomial, and for trinomial generated fields, delay of the modular reduction circuit and exponentiation circuits are small compared to pentanomial generated fields [3].

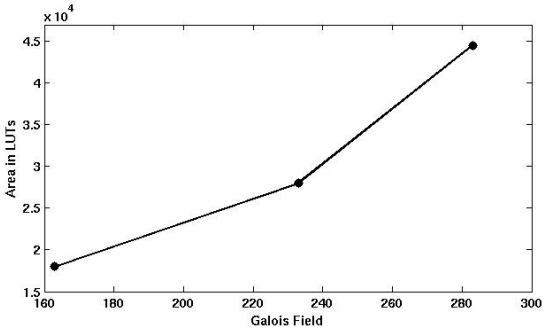

Figure 1: Galois Field vs Area in Virtex V

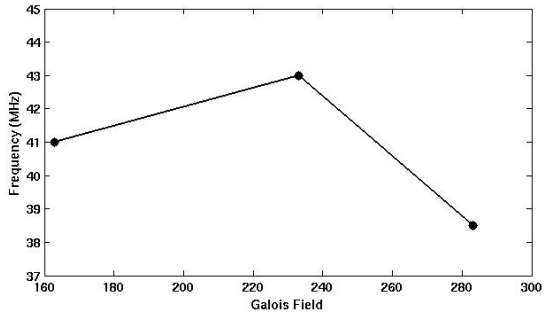

Figure 2: Galois Field vs Frequency in Virtex V

2.2 Software Testing

In this section we present the test results for the software implementations of PSEC-KEM. The Random and Kobliz curves were implemented with optimized finite field primitives in $GF(2^{283})$ in 64-bit processor architectures, hence we present timing reports for encryption and decryption operations in Intel 64 bit Core 2 Duo, 2.8 GHz processor. The implementation over OEF targets 32-bit and 64-bit platforms, so results are presented for that platform (Table 3).

2.2.1 Analysis of Software Performance

Here we discuss the major overheads of OEF implementation.

- Prime field arithmetic is more complex compared to operations in binary fields. In particular, the complexity of squaring in the OEF is $O(n^2)$, while in binary curves, squaring is done in linear time.
- The implementations in binary curves uses the highly efficient Lopez-Dahab finite field multiplication. The OEF implementations on the other hand use classical multiplication techniques in prime fields.

Elliptic curve	Field	Platform	Encryption		Decryption	
			Latency (μsec)	Throughput (encyptions/sec)	Latency (μsec)	Throughput (decryptions/sec)
Koblitz	$GF(2^{283})$	Intel Core2 Duo (64bit), 2.8GHz	2890	346	2910	343
Random	$GF(2^{283})$	Intel Core 2 Duo (64bit), 2.8GHz	5800	172	5800	172
OEF-ECP31M07K	$GF((2^{31}-1)^7)$	Intel Xeon (64bit), 2.33GHz	4407	226	4389	227
OEF-SECO305R	$GF((2^{61}-1)^5)$	Intel Xeon (64bit), 2.33GHz	5046	198	5204	192
OEF-SECO427R	$GF((2^{61}-1)^7)$	Intel Xeon (64bit), 2.33GHz	13487	74	13150	76
OEF-ECP31M07K	$GF((2^{31}-1)^7)$	Intel Core 2 Duo (32bit), 2.93GHz	7241	138	7215	138
OEF-SECO305R	$GF((2^{61}-1)^5)$	Intel Core 2 Duo (32bit), 2.93GHz	8762	114	8722	114
OEF-SECO427R	$GF((2^{61}-1)^7)$	Intel Core 2 Duo (32bit), 2.93GHz	22457	44	22400	44

Table 3: Computation time on Intel Processors

- Some operations in the PSEC KEM algorithm (ECP2OSP, OS2IP, PECP2OSP) are implemented with multi-precision arithmetic and have significant overheads. These functions can be easily implemented in the binary implementations.

Figure 3 compares the latency in the PSEC-KEM PSEC-KEM encryption with respect to the field size for the OEFs. The figure shows significant increase in the latency with the field size. This is mainly due to the $O(n^2)$ multiplication in the base field. All other operations grow linearly with the field size. Moreover, besides the scalar multiplication and the modular reduction, the remaining parts of the algorithm are independent of the size of the field.

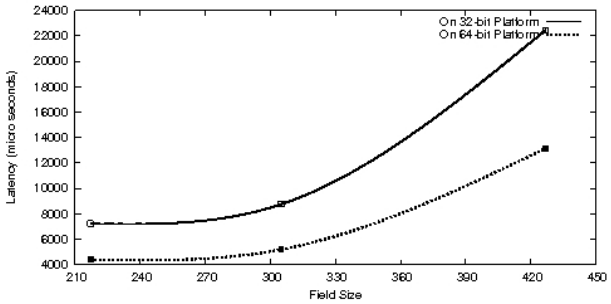

Figure 3: Field Size vs Latency of PSEC-KEM Encyption